



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS : A. Jung KIM et al.
SERIAL NO. : 10/634,700
FILED : August 5, 2003
FOR : METHOD FOR TRANSMITTING SECURITY DATA IN
ETHERNET PASIVE OPTICAL NETWORK SYSTEM

PETITION FOR GRANT OF PRIORITY UNDER 35 USC 119

MAIL STOP PATENT APPLICATION
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA. 22313-1450

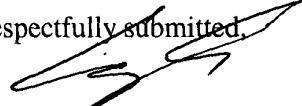
Dear Sir:

Applicant hereby petitions for grant of priority of the present Application on the basis of the following prior filed foreign Application:

<u>COUNTRY</u>	<u>SERIAL NO.</u>	<u>FILING DATE</u>
Republic of Korea	2002-46600	August 7, 2002

To perfect Applicant's claim to priority, a certified copy of the above listed prior filed Application is enclosed. Acknowledgment of Applicant's perfection of claim to priority is accordingly requested.

Respectfully submitted,


Steve S. Cha
Attorney for Applicant
Registration No. 44,069

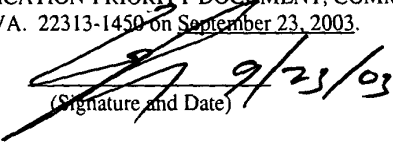
CHA & REITER
411 Hackensack Ave, 9th floor
Hackensack, NJ 07601
(201)518-5518

Date: September 23, 2003

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MS PATENT APPLICATION-PRIORITY DOCUMENT, COMMISSIONER FOR PATENTS, P. O. BOX 1450, ALEXANDRIA, VA. 22313-1450 on September 23, 2003.

Steve S. Cha, Reg. No. 44,069
Name of Registered Rep.)


(Signature and Date) 9/23/03



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Intellectual
Property Office.

출 원 번 호 : 10-2002-0046600
Application Number

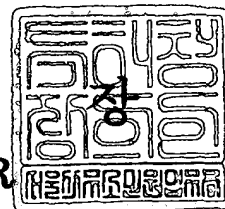
출 원 년 월 일 : 2002년 08월 07일
Date of Application AUG 07, 2002

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003 년 08 월 26 일

특 허 청
COMMISSIONER



1020020046600

출력 일자: 2003/8/29

	【서지사항】
【서류명】	서지사항 보정서
【수신처】	특허청장
【제출일자】	2003.07.16
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【사건과의 관계】	출원인
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	2003-001449-1
【사건의 표시】	
【출원번호】	10-2002-0046600
【출원일자】	2002.08.07
【발명의 명칭】	점대다 토폴로지의 네트워크에서 논리링크의 형성과 그 보안 통신 방법
【제출원인】	
【접수번호】	1-1-2002-0255126-18
【접수일자】	2002.08.07
【보정할 서류】	특허출원서
【보정할 사항】	
【보정대상 항목】	발명자
【보정방법】	정정
【보정내용】	
【발명자】	
【성명의 국문표기】	김아정
【성명의 영문표기】	KIM,A Jung
【주민등록번호】	660121-2037322
【우편번호】	140-731
【주소】	서울특별시 용산구 이태원2동 청화아파트 5동 805호
【국적】	KR

【발명자】**【성명의 국문표기】**

김진희

【성명의 영문표기】

KIM, Jin Hee

【주소】

경기도 수원시 팔달구 영통동 963-2 쌍용 아파트 544-707

【국적】

US

【발명자】**【성명의 국문표기】**

송재연

【성명의 영문표기】

SONG, Jae Yeon

【주민등록번호】

720523-2178211

【우편번호】

463-020

【주소】

경기도 성남시 분당구 수내동 양지마을 한양 아파트 514동 90 2호

【국적】

KR

【발명자】**【성명의 국문표기】**

임세윤

【성명의 영문표기】

LIM, Se Youn

【주민등록번호】

730815-1094428

【우편번호】

151-802

【주소】

서울특별시 관악구 남현동 1054-33 신원빌리지 302호

【국적】

KR

【취지】

특허법시행규칙 제13조·실용신안법시행규칙 제8조의 규정에의하여 위와 같 이 제출합니다. 대리인 이견주 (인)

【수수료】**【보정료】**

0 원

【기타 수수료】

원

【합계】

0 원

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2002.08.07
【국제특허분류】	H04J
【발명의 명칭】	점대다 토폴로지의 네트워크에서 논리링크의 형성과 그 보안 통신 방법
【발명의 영문명칭】	METHOD FOR CONNECTING LOGICAL LINK AND COMMUNICATING BY THE LOGICAL LINK IN POINT TO MULTIPOINT TOPOLOGY NETWORK
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	1999-006038-0
【발명자】	
【성명의 국문표기】	김아정
【성명의 영문표기】	KIM,A Jung
【주민등록번호】	660121-2037322
【우편번호】	140-731
【주소】	서울특별시 용산구 이태원2동 청화아파트 5동 805
【국적】	KR
【발명자】	
【성명의 국문표기】	김진희
【성명의 영문표기】	KIM,Jin Hee
【주소】	경기도 수원시 팔달구 영통동 963-2 쌍용 아파트 544-707
【국적】	US

【발명자】**【성명의 국문표기】**

송재연

【성명의 영문표기】

SONG, Jea Youn

【주민등록번호】

720523-2178211

【우편번호】

463-020

【주소】경기도 성남시 분당구 수내동 양지마을 한양아파트
514동 902호**【국적】**

KR

【발명자】**【성명의 국문표기】**

임세윤

【성명의 영문표기】

LIM, Se Youn

【주민등록번호】

730815-1094428

【우편번호】

151-802

【주소】서울특별시 관악구 남현동 1054-33 신원빌리지 302
호**【국적】**

KR

【취지】특허법 제42조의 규정에 의하여 위와 같이 출원합
니다. 대리인
이건주 (인)**【수수료】****【기본출원료】**

20 면 29,000 원

【가산출원료】

8 면 8,000 원

【우선권 주장료】

0 건 0 원

【심사청구료】

0 항 0 원

【합계】

37,000 원

【요약서】**【요약】**

가. 발명이 속하는 기술분야

본 발명은 점대다 토폴로지의 네트워크의 보안통신에 관한 것으로, 특히 이더넷 수동형광가입자망에서 논리 링크를 형성하고 이를 단위로 한 보안 통신 방법에 관한 것이다.

나. 발명이 해결하고자 하는 기술적 과제

본 발명의 목적은 이더넷 수동형광가입자망구조에서 802.1d bridge와의 비호환성을 극복하고 사용자-사용자간(End User-to-End User)의 통신이나 멀티 서비스를 지원할 수 있는 논리링크와 그 연계 가상 링크(virtual link) 형성을 구현하기 위한 이더넷 프레임 구조를 제공하고 이러한 링크를 단위로 한 이더넷 수동형광가입자망에서의 보안 통신 방법을 제공함에 있다.

다. 발명의 해결방법의 요지

본 발명은 하나의 OLT와 상기 OLT에 접속되는 적어도 하나의 ONU로 구성되는 이더넷 수동형광가입자망에서 점대점 에멀레이션 상의 논리링크를 형성하고 이러한 개개 링크 상에 메시지를 암호화하여 보안통신을 수행하는 방법에 있어서, 상기 OLT와 ONU 간에서 보안통신을 수행하기 위한 클리어 수동형광가입자망 태그 헤더 필드를 포함하는 이더넷 프레임을 생성하는 과정과, 상기 생성된 이더넷 프레임을 전송하는 과정으로 이루어짐을 특징으로 한다.

라. 발명의 중요한 용도

이더넷 수동형광가입자망에서의 보안을 위해 사용된다.

【대표도】

도 4

【색인어】

수동형광가입자망, 가상 랜, 암호화

【명세서】

【발명의 명칭】

점대다 토폴로지의 네트워크에서 논리링크의 형성과 그 보안 통신 방법
{METHOD FOR CONNECTING LOGICAL LINK AND COMMUNICATING BY THE LOGICAL LINK IN
POINT TO MULTIPOINT TOPOLOGY NETWORK}

【도면의 간단한 설명】

도 1은 일반적인 수동형광가입자망(Passive Optical Network, PON)의 물리적 구조를 도시한 도면,

도 2는 본 발명의 일 실시 예에 따른 이더넷 수동형광가입자망 이더넷 프레임의 메시지 포맷을 도시한 도면,

도 3은 본 발명의 일 실시 예에 따른 도면으로, 클리어 수동형광가입자망 태그 헤더 포맷을 도시한 도면,

도 4는 본 발명의 일 실시 예에 따른 도면으로, 이더넷 수동형광가입자망의 프로토콜 스택을 도시한 도면,

도 5는 본 발명의 일 실시 예에 따른 도면으로, 이더넷 수동형광가입자망의 프로토콜 스택 중 특히 암호화 계층을 도시하는 도면.

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <6> 본 발명은 이더넷 수동형광가입자망에 관한 것으로, 특히 이더넷 수동형광 가입자망에서 논리 링크의 형성과 보안 통신 방법에 관한 것이다.
- <7> 도 1은 일반적인 수동형광가입자망의 물리적 망 구조를 도시하고 있다.
- <8> 도 1에 도시된 바와 같이, 수동형광가입자망은 하나의 OLT(100)와 상기 OLT(100)에 접속되는 적어도 하나의 ONU(110-1 내지 110-3)로 구성된다. 도 1에 는 하나의 OLT(100)에 3개의 ONU들(110-1 내지 110-3)이 접속된 예가 도시되어 있다. 상기 ONU들(110-1 내지 110-3)에는 각각 적어도 하나의 End User(사용자, 네트워크 장치)들(120-1 내지 120-3)이 접속될 수 있다. 상기 사용자들(120-1 내지 120-3)이 전송하는 데이터들(131 내지 133)이 ONU들(110-1 내지 110-3)을 거쳐 OLT(100)로 전송된다. 한편, 상기 사용자들(120-1 내지 120-3)이 송신하는 데이터들에 참조부호를 부가함에 있어 각 전송 구간에 따라 다른 부호를 붙였으나(예컨대, 131-1, 131-2, 131-3) 각 구간의 구분이 필요치 않을 시는 하나의 대표번호를 칭함으로서 그 데이터를 가리키도록 한다(예컨대, '131-1, 131-2, 131-3'을 '131'로 칭함). 도 1에 도시된, 802.3 이더넷 프레임을 점대 다점 구조의 네트워크를 통해 전송하는 이더넷 수동형광가입자망(Ethernet Passive Optical Network, EPON)구조에서, 상향 전송의 경우 TDM(Time Division Multiplexing) 방식으로 전송하고, 하향전송의 경우 'Broadcast and selection'

를에 의해 전송한다. 즉, 상향 전송 시에는 각 ONU들(110-1 내지 110-3)의 데이터가 멀티플렉싱되어 OLT(100)로 전송되고, 하향 전송 시에는 OLT(100)가 브로드캐스트하는 데이터를 수신한 ONU들(110-1 내지 110-3)이 상기 데이터 중 자신이 수신할 데이터만을 선택하여 수신한다.

<9> 그런데, 이때 다음과 같은 문제점이 야기된다. 첫째, 802.1d 와의 비호환성으로 인해 L2 내에서 ONU들(110-1 내지 110-3) 끼리는 피어(peer)측, 같은 계층에서 통신이 불가능하므로 다른 ONU(110-1 내지 110-3)에 연결되어 있는 사용자(120-1 내지 120-3)와는 L2 내에서 통신이 불가능하여 피어투피어(peer-to-peer) 통신이 불가능하다. 이를 해결하기 위해 논리링크 아이디(Logical Link ID, LLID)를 이용하여 점대점에물레이션(point-to-point emulation)을 하여 피어투피어 통신이 가능케 할 수 있다.

<10> 둘째, 보안에 대한 문제가 있다. 상술한 바와 같이 하향 전송 시 'Broadcast and Selection' 방식을 선택함으로써 인해, 수동형광가입자망에서 하향의 메시지는 모든 ONU들(110-1 내지 110-3)에게 전송되고 그중 해당하는 ONU들(110-1 내지 110-3)만이 메시지를 필터링해서 받는 구조이므로 보안성이 취약하다. 또한, 상향 링크에 대해 인증 받지 않은 ONU(110-1 내지 110-3)의 네트워크 접근이 가능하고, 수동형광가입자망 상의 임의의 ONU(110-1 내지 110-3)가 다른 ONU(110-1 내지 110-3)인양 위장하여 'Denial of Service' 어택이나 자료 및 자원의 접근이 가능하므로 인증의 절차가 필요하다. 따라서 점대 다점 구조의 네트워크에서 각 ONU(110-1 내지 110-3)나 논리링크 아이디에 대하여 인증절차를

통한 서로 다른 키를 분배하여 메시지를 암호화하는 절차를 통하여 하향신호에 대해 프라이버시를 보장하고 상향신호에 대해 메시지에 대한 인증을 할 수 있다.

<11> ATM 수동형광가입자망 용 암호의 기술은 이미 표준화가 완료되어 있는 상태로써 그 내용은 ITU-T G.983.1 에 기술되어 있다. 그러나 이더넷 프레임의 수동형광가입자망이라는 피지컬 플랜트(physical plant)를 통하여 전송하는 이더넷 수동형광가입자망의 암호기능 및 구현 방법은 현재 정의되어 있지 않다.

<12> 이에 따라, 이더넷 수동형광가입자망에 피어 투 피어(peer-to-peer)통신을 가능케 하는 방안으로서 논리링크 아이디를 이용한 점대점 에뮬레이션(point-to-point emulation)을 구현하기 위해 논리링크 아이디를 이더넷 프레임의 프리앰블(preamble)에 넣어 프로세싱하는 방안이 제안되었다(IEEE802.3ah July meeting). 이때 보안 서비스(security service) 제공 역시 프리앰블에 암호화(encryption)나 보안 서비스에 대한 태그(tag)를 첨가함으로서 논리링크 아이디별로 보안 서비스를 차별화 하여 수행할 수 있다.

<13> 그러나, 상기 방안은 하드웨어의 변경을 필요로 하기 때문에 이것은 다른 토폴로지(topology)를 가지는 네트워크와의 호환성이 결여되어 있다.

<14> 또, 프리앰블의 프로세싱을 위해 RS 계층에서 암호화(encryption)를 수행할 경우, 암호 알고리즘을 이용하여 메시지를 암호화함에 있어 메시지의 인증을 위해 메시지 뿐 아니라 FCS(frame check sequence, 프레임 체크 시퀀스)까지 암호화하는 방식이 대두되는데 이 방식은 링크 관리(link management) 상의 문제를 야기시킨다. 즉, 에러가 있는 노이지 링크(noisy link)에 대해서 FCS 체크 에러가

발생하였을 시, 상기 에러가 링크(link)나 다른 장치(device) 결함에 의한 에러인지 아니면 인증되지 않은 메시지로 인한 에러인지 구별이 불가능하게 된다.

<15> 또, 상기 방안을 이용할 시, QoS(Quality of Service)나 SLA(Service Level Agreement)의 구현에 있어서도 문제점이 발생한다. 하나의 ONU(110-1 내지 110-3)에 다수의 논리링크 아이디를 부여하여 서비스 차별(service segregation)이나 트래픽 차별(traffic segregation)을 수행하려는 경우는 가드 밴드(guard band)의 점유율이 높아 링크 이용(link utilization) 상 비효율적이 되고 ONU들(110-1 내지 110-3)간의 스위칭에 있어 많은 문제점을 야기한다.

<16> 또한, 논리링크 아이디와 가상 랜(Virtual LAN, VLAN) 기법을 연계시켜 서비스 차별이나 트래픽 차별을 수행할 경우는 가상 랜 스페이스(space)의 크기에 한정이 있고, 각기 서로 다른 서비스 제공자(service provider)가 지원하는 가상 랜이 혼재할 경우 그러한 구획(compartment)을 지원하지 않는 방식에서는 가상 랜간의 상호운용성(interoperability)이 결여되어 하나의 물리 토폴로지(physical topology)상에서 수행하기 어렵다.

【발명이 이루고자 하는 기술적 과제】

<17> 따라서 상기와 같은 문제점들을 해결하기 위한 본 발명의 목적은 이더넷 수동형광가입자망구조에서 802.1d bridge와의 비호환성을 극복하고 사용자-사용자 간(End user-to-End user)의 통신이나 멀티 서비스를 지원할 수 있는 논리링크와 그 연계 가상 링크(virtual link) 형성을 구현하기 위한 이더넷 프레임 구조를

제공함으로서 이더넷 수동형광가입자망에서의 보안 통신을 이루는 단위 및 보안 통신 방법을 제공함에 있다.

<18> 본 발명의 다른 목적은 점대 다점 구조를 가진 이더넷 수동형광가입자망 구조에서 가지는 보안의 취약성을 보완하기 위해 암호화를 통한 이더넷 수동형광가입자망에서의 보안 통신 방법을 제공함에 있다.

<19> 본 발명의 또 다른 목적은 802.1d, 802.10 과 호환성이 있으면서 QoS, SLA 등이 가능하고 보안 및 데이터의 무결성여부(data integrity), 데이터의 근원지에 대한 무결성여부(data origin integrity) 등을 체크할 수 있는 이더넷 수동형광가입자망에서의 보안 통신 방법을 제공함에 있다.

<20> 상기 목적을 달성하기 위한 본 발명은 하나의 OLT와 상기 OLT에 접속되는 적어도 하나의 ONU로 구성되는 이더넷 수동형광가입자망에서 논리링크를 통한 보안통신을 수행하는 방법에 있어서, 상기 OLT가 상기 OLT와 ONU 간에서 보안통신을 수행하기 위한 클리어 수동형광가입자망 태그 헤더 필드를 포함하는 이더넷 프레임을 생성하는 과정과, 상기 생성된 이더넷 프레임을 전송하는 과정으로 이루어짐을 특징으로 한다.

【발명의 구성 및 작용】

<21> 이하 본 발명의 바람직한 일 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 하기에서 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한

구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다.

<22> 본 발명은 하나의 OLT(Optical Line Terminal)(100)와 상기 OLT(100)에 연결되는 하나 이상, 다수의 ONU(Optical Network Unit)(110-1 내지 110-3)로 구성된 점대 다점(point-to-multipoint) 구조의 이더넷 수동형광가입자망에서 점대점에 물레이션을 통한 논리링크를 형성하고 상기 논리링크를 배타적인 사적 링크로 형성하기 위해 각각의 논리링크를 보안 서비스의 그랜놀래리티(granularity)로 하여 암호화함으로서 비밀 데이터의 전송이 가능하게 한다. 더불어 본 발명은 가상 랜 기법과 연동하여 물리적 네트워크에 논리적 가상 랜 토폴로지를 구현하고 나아가 QoS나 SLA가 가능한 토대를 제공하는 기법이다.

<23> 이를 위한 본 발명의 특징은 점대점 에물레이션을 수행하기 위한 논리링크 아이디를 이더넷 프레임 내에 삽입함에 있다. 상기 이더넷 프레임 내에 삽입된 아이디를 여러 가상 랜에 대한 그룹 ID와 레이트 한정(rate limiting) 및 서비스 차별(service segregation) 등을 수행하기 위해 가상 랜이나 이와 유사한 목적의 ID의 결합체로 간주하여 암호 메커니즘을 수행한다. 아울러, 이더넷 프레임 내에 데이터 무결성여부 체크(data integrity check)나 데이터 근원지 무결성여부 체크(data origin integrity check)등을 수행할 필드를 삽입하고 이를 메시지와 함께 암호화한다.

<24> 도2는 본 발명의 일 실시 예에 따른 이더넷 메시지 프레임 포맷이다.

- <25> 도 2의 PA, DA, SA, FCS는 각각 IEEE 802.3에서 정의한 프리앰블(preamble), 목적지 주소(destination address), 발신지 주소(source address), 프레임 체크 시퀀스(frame check sequence)를 의미한다.
- <26> 본 실시 예에서는 802.3 MAC 프레임 상에서 MAC 헤더 뒤에 에플레이션과 보안에 대한 태그가 삽입된다.
- <27> 도 3은 상기 도 2에 도시된 이더넷 메시지 프레임 포맷 중 특히 클리어 PON(수동형광가입자망) 태그 헤더를 도시하는 도면이다.
- <28> 도 3에 도시된 바와 같이, 클리어 PON 태그 헤더(clear PON tag header)(206)는 상기 이더넷 프레임이 특수 태그드 프레임(tagged frame)임을 나타내는 데지그네이터(designator)(300)와 PON 관련 아이디(PAID, PON Association ID) 필드(302), 그 외에 부가되는 선택적(optional) 필드(304)로 구성된다. 상기 도 2에는 선택적 필드(304)로서 MDF(Management Defined Field)가 도시되어 있다.
- <29> 상기 태그드 프레임 데지그네이터(tagged frame designator, 이하 '데지그네이터'라 칭함)(300)의 예로는 802.10과의 호환성을 위해 2바이트의 예비 LSAP(Link service access point)인 16진수의 '0x0A0A'와 1바이트의 UIC(Unnumbered Information Control; ISO/IEC8802-2:1998)의 값 '0x03'을 결합(concatenated)한 값을 지정하여 사용할 수 있다. PAID 필드(302)는 각 ONU(110-1 내지 110-3)들을 구별하여 피어투피어 통신이 가능하게 하고 각 ONU(110-1 내지 110-3)에 대한 서비스를 사용자 그룹별로 구별하여 서비스 차별이나 트래픽 차별이 가능하도록 하는 식별자를 의미한다. 상기 식별자는 각기

다른 키가 주어져 보안 서비스를 수행하는 엔티티(entity)로 간주되어지기도 한다.

<30> 한편, 상기 도 3에는 상기 PAID(302)의 구성의 일 예가 함께 도시되어 있다. 상기 PAID(302)는 ONU(110-1 내지 110-3) 혹은 서로 다른 서비스 제공자와 같은 관리 엔티티(management entity)를 구분 짓는 LLID 필드(312)와 상기 LLID 필드(312)를 그룹 ID로 하여 하나의 ONU(110-1 내지 110-3)가 관장하는 다수의 엔티티에 대한 SID로 구성된다. 관리 엔티티가 관장하는 SID의 숫자에 따라서 여러 가지 클래스로 LLID 필드(312)와 SID 필드(314)의 개수를 제한시킬 수 있는데, 802.10과의 호환을 위해서는 3비트의 그룹 비트(group-bits)의 값 '101'에 17bit의 LLID 필드(312), 12bit의 SID 필드(314)를 사용함이 바람직하다. 이 때 LLID 필드(312)는 다시 브로드캐스트/유니캐스트(broadcast/unicast)를 나타내는 1비트의 모드 비트(mode bit)와 16비트의 실제 LLID(312)로 구성되어질 수도 있다. SID 필드(314)는 기존의 가상 랜기법을 사용할 경우 가상 랜 아이디에 해당한다.

<31> 따라서, 상기와 같은 경우, 경우 65536개의 서로 다른 ONU(110-1 내지 110-3)와 관리자의 조합에 대해 4096의 서로 다른 가상 랜을 지원할 수 있다. 만약 목적지가 멀티캐스트 그룹 주소일 경우 PAID 필드(302)는 그 그룹의 모든 사용자들에게 공통의 값을 가진 값으로 정해질 수 있다. 즉 관리 엔티티는 멀티캐스트 그룹 어드레스의 경우 단일의 멀티캐스트 그룹 PAID를 할당하고 그 그룹 멤버들에게만 일정한 키를 주어 보안 서비스를 수행함으로써 멀티캐스트 데이터에 대한 관리를 할 수 있다.

- <32> MDF(management defined field)(304)는 선택적 필드로서 여러 가지 MIB(Management Information Base)에 대한 정보나 관련 프로토콜에 대한 정보 등을 담을 수 있다.
- <33> 한편, 상기 도 2에 도시된 프로텍티드 태그 헤더(protected tag header) 필드(208)는 선택적이며 암호화되는 필드로서, 데이터 근원지(data originating station)에 대한 무결성여부 체크(integrity check), 보안 레벨(security label), 프래그먼트 아이디(fragment ID), 플래그(flag) 등의 선택적인 정보를 전달할 수 있다.
- <34> 패드(PAD) 필드(212)는 역시 선택적인 필드로서, 시스템이 사용하는 암호 알고리즘(confidentiality algorithm)이나 무결성여부 알고리즘(integrity algorithm)이 일정 길이의 데이터를 필요로 할 경우 그에 따라서 첨가될 수도 있고 아닐 수도 있다. 상기 패드 필드(212)는 암호화상의 오씨비(OCB) 모드나 씨에스티(CST) 모드 등, 패킷의 길이를 보존하는 메커니즘을 사용할 경우는 필요 없다. 한편, 패딩(padding)이 필요한 알고리즘의 경우 상기 패드 필드(212)의 마지막에 패드의 길이를 표시하는 필드가 부가되어야 한다.
- <35> ICV(Integrity Check Value) 필드(214)는 메시지 결함여부 체크(message integrity check)를 위해 사용된다. 예컨대, 암호화 알고리즘으로 AES(Advanced Encryption Standard)를 사용한 오씨비 모드를 적용할 경우 ICV 필드(214)의 값은 4바이트나 10바이트의 체크섬(check sum)에 해당한다. 무결성여부 체크의 범위는 프로텍티드 태그 헤더 필드(208), PDU(Packet Data Unit, 패킷 데이터 유닛) 필드(210), 패드 필드(212)에 대해서 적용될 수 있다.

- <36> 도4는 본 발명의 일 실시 예에 따른 도면으로, 이더넷 수동형광가입자망에서 보안 통신 기능을 수행하는 계층을 프로토콜 스택 상에 표시한 것이다.
- <37> 도 5는 본 발명의 일 실시 예에 따른 도면으로, 특히 상기 도 4에 도시된 이더넷 수동형광가입자망의 프로토콜 스택 중 특히 암호화 계층의 프리미티브(Premitive)를 도시하는 도면이다.
- <38> 먼저 다수의 PAID 필드(302)는 서비스/트래픽 차별이 수행되는 개체를 구별짓는데 사용되며, 이는 각기 다른 키가 주어진 엔티티를 의미하기도 한다. 또는 한 개의 ONU(110-1 내지 110-3)에 해당하는 그룹 ID마다 각기 다른 키를 주고 서비스/트래픽 차별을 SID별로 수행할 수도 있다.
- <39> 보안 서비스가 제공되지 않을 때는 데지그네이터 필드(300)에 802.10 가상 랜 프레임임을 가리키는 특정 값을 표기한 후 PAID 필드(302) 중 SID 필드(314)에 실제 가상 랜 ID를 적는다. 이를 통해 암호화에 대한 오버헤드 없이 가상 랜 스페이스를 서비스 제공자나 ONU(110-1 내지 110-3) 별로 확장하여 사용할 수 있게 되어 QoS, SLA, 전송률 한정 등이 가능해진다.
- <40> 단, 이때 암호화를 하느냐 안 하느냐에 따라 암호화 프로세싱 타임으로 인해 실제 패킷이 왕복 전송을 하는데 걸리는 시간인 RTT(Round Trip Time)값에 변화를 가져올 수 있다. 따라서 암호화 엔진은 패킷의 길이에 무관하게 프로세싱 타임이 소요되도록 패러렐 프로세싱(parallel processing) 함이 바람직하다. 또, 암호화되지 않은(encryption-disable) 패킷의 경우도 고정된 RTT를 보장하기 위해 암호화 프로세스와 동일한 일정 지연을 초래하도록 조정되어야 한다.

<41> 보안 서비스를 지원한 경우에는, 먼저 메시지의 전송은 MAC 클라이언트 (client)(400-1, 400-2)에서 트리거 되어 암호화 계층(encryption layer)(404)으로 전송된다. 이때 MAC 상위 계층(402)에서 클리어 태그 헤더(206)가 삽입된다. 이후 도 5에 도시된 바와 같이, ENC_UNIDATA.request(505)로 DA,SA, m_sdu, 등이 암호화 계층(404)으로 전달된다. 암호화 계층(404)에서는 암호화 할지의 여부에 따라 보안 메커니즘에 연관된 프로텍티드 태그 헤더 필드(208)와 패드 필드(212)를 삽입한 후 무결성여부 체크를 통해 무결성여부 체크 필드를 삽입하고, 상기 프로텍티드 태그 헤더 필드(208), 패드 필드(212) 및 결함여부 체크 필드 영역과 ICV 필드(214) 전체에 대해서 메시지와 함께 암호화를 수행한다. 즉, 이더넷 프레임 상에서 암호화되는 영역은 프로텍티드 태그 헤더 필드(208)부터 ICV 필드(214)까지이다.

<42> 도 5의 MA_UNIDATA.request(501)는 상기 도 2에 정의된 이더넷 메시지 프레임 포맷에서 FCS 필드(216)를 제외한 이더넷 프레임이 된다.

<43> MAC 계층(406)에서는 상기 암호문을 포함한 MAC 프레임에 대한 물리적 에러 발생여부를 체크하기 위한 FCS 필드(216)를 첨가한다. MAC 계층(406)은 수신된 메시지에 대해서 MAC 계층(406)으로 전송된 이더넷 프레임의 암호화한 부분을 포함한 모든 이더넷 프레임 영역(DA~ICV)(202 내지 214)에 대해 FCS 체크를 수행한다. 이러한 방식으로 전송된 프레임을 수신한 MAC 계층(406)은 자신이 수행한 FCS 결과 값과 상기 전송된 이더넷 프레임에 포함된 FCS 필드(216)의 수치를 비교한 후 그 결과를 수신 상태(receive_status) 신호로 상위 계층에 전달한다. 이때 MAC 계층(406)은 FCS 필드(216)를 제거한다. 이후 전송 시와 역으로 복호

화(description)를 수행한 후 무결성여부 체크를 수행하고, 그 값을 ICV 필드(214)의 값과 비교하여 일치하지 않을 경우 메시지 무결성여부 카운트(message integrity break count)에 기록한다.

<44> 암호화된 암호 처리된 영역의 체크섬 값이 FCS의 값과 일치하여 FCS 체크를 통과한 경우는 링크나 프로세스 상의 결함으로 인한 에러가 없음을 의미한다. 또, 이후 복호화 과정을 거쳐 복호화된 평문의 ICV 영역의 체크섬 값이 ICV의 값과 일치할 경우 올바른 키로 암호화되었다는 것을 의미하므로 이는 메시지의 무결성여부를 입증한다. 상술한 바와 같이, FCS 체크는 링크나 프로세스 상의 에러를 체크하기 위한 것이고, ICV 체크는 이더넷 프레임에 포함된 메시지나 메시지 근원지 무결성여부를 체크하기 위한 것이다.

<45> 이 후 패드 필드(212)와 암호화 태그, ICV 필드(214) 등을 제거하고 PAID 필드(302)를 포함한 클리어 태그 헤더 필드(206)와 PDU 필드(210), DA 필드(202), SA 필드(204)를 MAC 클라이언트(400-1, 400-2)까지 전송한다.

<46> 상술한 바와 같이, 본 발명의 실시 예에서는 논리적 링크에 해당하는 LLID 필드(312)를 이더넷 메시지 프레임에 포함시켜 전송함으로써 물리 계층에 대해 독립적인(PHY-independent) 기법을 구현할 수 있다. 따라서, 기존의 물리 계층에 해당하는 어떠한 물리적 환경이나 네트워크의 토폴로지에 대해서도 호환성을 가지게 된다. 또, 각 ONU(110-1 내지 110-3)나 서비스 제공자에 대해 LLID 필드(312)를 그룹 ID로 부여함으로써 가상 랜 공간을 확장할 수 있고, 가상 랜간의 상호운용성을 구현할 수 있다. 이와 같이 PAID 필드(302)를 이용함으로써 필요에 따라 서비스 차별, 트래픽 차별, 전송률 한정(rate limiting) 등을 구현할

수 있는 기반을 제공할 수 있게 된다. 또, 본 실시 예에서는 LLID 필드(312)나 PAID 필드(302)별로 키 관리를 수행하여 데이터 무결성여부, 데이터 근원지 무결성여부, 기밀성 등의 보안 서비스가 가능해진다.

<47> 한편, 상기 본 발명을 설명하기 위해 사용한 실시 예나 구체적인 특정 수치 등은 본 발명의 이해를 돕기 위해 사용된 것일 뿐, 본 발명이 이로 인해 한정되지 않음은 자명하다.

【발명의 효과】

<48> 상술한 바와 같은 본 발명을 수행함으로써 이더넷 수동형광가입자망에서 물리계층에 독립적인, 어떠한 물리환경이나 토폴로지에 대해서도 호환성이 있는 신호 처리기반을 형성하고, 이를 기반으로 보안통신을 수행할 수 있다. 또한 가상 그룹 ID 개념을 첨가하여 가상 랜 스페이스를 확장할 수 있고, 가상 랜간의 상호운용성을 구현할 수 있다. 서비스 차별, 트래픽 차별, 전송률 한정 등을 구현할 수 있고, 이를 사적인 링크화할 수 있는 보안 서비스가 가능하다.

【특허청구범위】**【청구항 1】**

하나의 OLT(Optical Line Terminal)와 상기 OLT에 접속되는 적어도 하나의 ONU(Optical Network Unit)로 구성되는 이더넷 수동형광가입자망에서 논리링크를 형성하고 이에 대한 보안통신을 수행하는 방법에 있어서,

상기 OLT가 상기 OLT와 ONU 간에서 보안통신을 수행하기 위한 논리링크 아이디를 포함하는 이더넷 프레임을 생성하는 과정과,

상기 생성된 프레임을 전송하는 과정으로 이루어짐을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 2】

제 1항에 있어서, 상기 이더넷 수동형광가입자망에서의 이더넷 프레임은,

목적지 주소를 나타내는 DA(Destination Address) 필드와,

발신지 주소를 나타내는 SA(Source Address) 필드와,

논리링크 아이디를 포함하는 클리어 수동형광가입자망 태그 헤더 필드와 데이터 필드를 포함하도록 구성됨을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 3】

제 2항에 있어서, 상기 클리어 수동형광가입자망 태그 헤더 필드는,

데지그네이터 필드와,

논리링크 아이디를 포함하는 PAID(PON Association ID) 필드를 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 4】

제 3항에 있어서,

상기 클리어 수동형광가입자망 태그 헤더 필드는 MDF(Management Defined Field) 필드를 더 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 5】

제 1항에 있어서, 상기 PAID 필드는,

상기 ONU에 적어도 하나 이상 부가된 논리적 링크를 나타내는 LLID(Logical Link ID) 필드를 포함하도록 구성됨을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 6】

제 5항에 있어서, 상기 PAID 필드는,

클래스를 나타내는 플래그 필드와,

SID 필드를 더 포함하도록 구성됨을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 7】

제 6항에 있어서,

상기 LLID는 ONU나 서비스 제공자별로 구별지을 수 있는 구별자로 할당될 수 있음을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 8】

제 6항에 있어서,

상기 SID는 임의의 ONU나 서비스 제공자에 대해 가상 랜 ID 등을 이용하여 다시 소그룹으로 나눌 수 있는 구별자로서 할당될 수 있음을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 9】

제 7항에 있어서,

상기 LLID로 구별지어진 그룹의 멤버들에게만 일정한 키를 할당할 수 있음을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 10】

제 8항에 있어서,

상기 LLID와 SID를 포함한 전체 PAID로 구별지어진 그룹의 멤버들에게만 일정한 키를 할당할 수 있음을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 11】

제 2항에 있어서,

상기 프레임은 ICV(Integrity Check Value) 필드를 더 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 12】

제 2항에 있어서,

상기 프레임은 프로텍티드 헤더 필드를 더 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 13】

하나의 OLT와 상기 OLT에 접속되는 적어도 하나의 ONU로 구성되는 이더넷 수동형광가입자망에서 논리링크를 형성하고 이에 대한 보안통신을 수행하는 방법에 있어서,

MAC(Medium Access Control) 클라이언트가 보낸 이더넷 메시지 프레임에 클리어 태그 헤더를 삽입하여 암호화 계층으로 전송하는 제 1과정과,

암호화 계층이 상기 이더넷 메시지 프레임 중 PDU(Packet Data Unit) 필드를 암호화하는 제 2과정을 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 14】

제 13항에 있어서,

상기 제 2과정에서 암호화시 사용하는 암호화 알고리즘에 따라 상기 이더넷 메시지 프레임에 패드 필드를 더 삽입함을 특징으로 하는 이더넷 수동형광가입자망의 보안 통신 방법.

【청구항 15】

하나의 OLT와 상기 OLT에 접속되는 적어도 하나의 ONU로 구성되는 이더넷 수동형광가입자망에서 논리링크를 형성하고 이에 대한 보안통신을 수행하는 방법에 있어서,

MAC 클라이언트가 보낸 이더넷 메시지 프레임에 클리어 태그 헤더를 삽입하여 암호화 계층으로 전송하는 제 1과정과,

암호화 계층이 상기 이더넷 메시지 프레임 중의 PDU 필드에 대해 무결성여부 체크를 수행 후 무결성여부 체크 필드를 삽입하는 제 2과정과,

암호화 계층이 상기 PDU 필드 및 무결성여부 체크 필드를 암호화하는 제 3 과정을 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 16】

하나의 OLT와 상기 OLT에 접속되는 적어도 하나의 ONU로 구성되는 이더넷 수동형광가입자망에서 논리링크를 형성하고 이에 대한 보안통신을 수행하는 방법에 있어서,

MAC 클라이언트가 보낸 이더넷 메시지 프레임에 클리어 태그 헤더를 삽입하여 암호화 계층으로 전송하는 제 1과정과,

암호화 계층이 상기 이더넷 메시지 프레임에 프로텍티드 태그 헤더 필드를 삽입하는 제 2과정과,

암호화 계층이 프로텍티드 태그 헤더 및 상기 이더넷 메시지 프레임 중의 PDU 필드에 대해 무결성여부 체크를 수행 후 무결성여부 체크 필드를 삽입하는 제 3과정과,

암호화 계층이 상기 프로텍티드 태그 헤더, PDU 필드 및 무결성여부 체크 필드를 암호화하는 제 4과정을 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 17】

하나의 OLT와 상기 OLT에 접속되는 적어도 하나의 ONU로 구성되는 이더넷 수동형광가입자망에서 논리링크를 형성하고 이에 대한 보안통신을 수행하는 방법에 있어서,

MAC(Medium Access Control) 클라이언트가 보낸 이더넷 메시지 프레임에 클리어 태그 헤더를 삽입하여 암호화 계층으로 전송하는 제 1과정과,

암호화 계층이 상기 이더넷 메시지 프레임 중 PDU(Packet Data Unit) 필드를 암호화하는 제 2과정과,

상기 암호화 계층으로부터 상기 암호화된 필드들을 포함하는 MAC 프레임을 전송 받고, 상기 프레임에 대해 에러 발생여부를 체크하는 FCS(Frame Check Sequence) 필드를 더 삽입하는 제 3과정을 더 포함함을 특징으로 하는 이더넷 수동형광가입자망의 보안 통신 방법.

【청구항 18】

하나의 OLT와 상기 OLT에 접속되는 적어도 하나의 ONU로 구성되는 이더넷 수동형광가입자망에서 논리링크를 통한 보안통신을 수행하는 방법에 있어서,

수신되는 메시지 프레임에 대해 MAC 계층이 FCS 체크를 수행하는 제 1과정과,

암호화 계층에서 상기 프레임에 대해 복호화를 수행하는 제 2과정과,

상기 복호화된 프레임에 대해 무결성여부 체크를 수행하는 제 3과정과,

상기 체크를 통해 에러 및 결함이 없는 것으로 판단된 프레임에 대하여 패드 필드, 암호화 태그 필드, ICV 필드를 적어도 포함하는 필드들을 제거하는 제 4과정과,

상기 필드들이 제거된, PAID와 PDU(Packet Data Unit), DA, SA를 맥 클라이언트로 전송하는 제 5과정을 포함함을 특징으로 하는 이더넷 수동형광가입자망에서의 보안 통신 방법.

【청구항 19】

제 18항에 있어서,

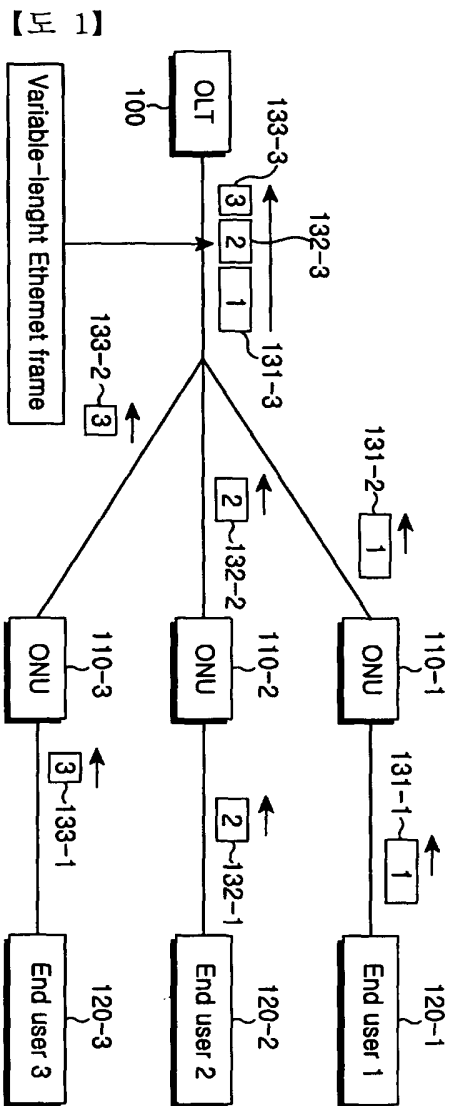
상기 제 1과정의 FCS에 있어서, FCS 결과 값과 상기 프레임의 FCS 필드의 체크섬 값이 일치하는 경우 에러가 없음으로 판단함을 특징으로 하는 이더넷 수동형광가입자망의 보안 통신 방법.

【청구항 20】

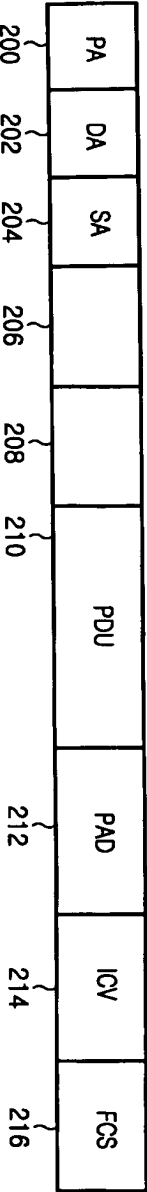
제 18항에 있어서,

제 3과정에서의 상기 무결성여부 체크 결과 값이 상기 프레임의 ICV 필드의 체크섬 값과 일치하는 경우 메시지나 메시지 근원지에 결함이 없음으로 판단함을 특징으로 하는 이더넷 수동형광가입자망의 보안 통신 방법.

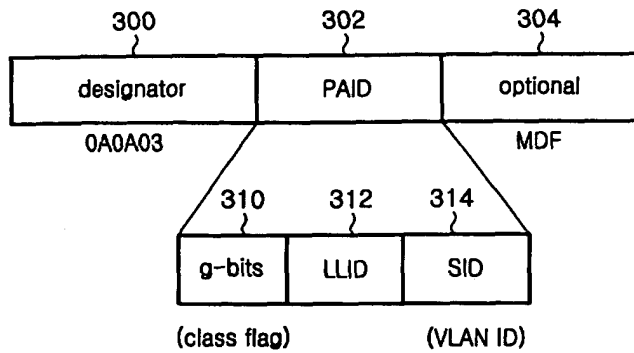
【도면】



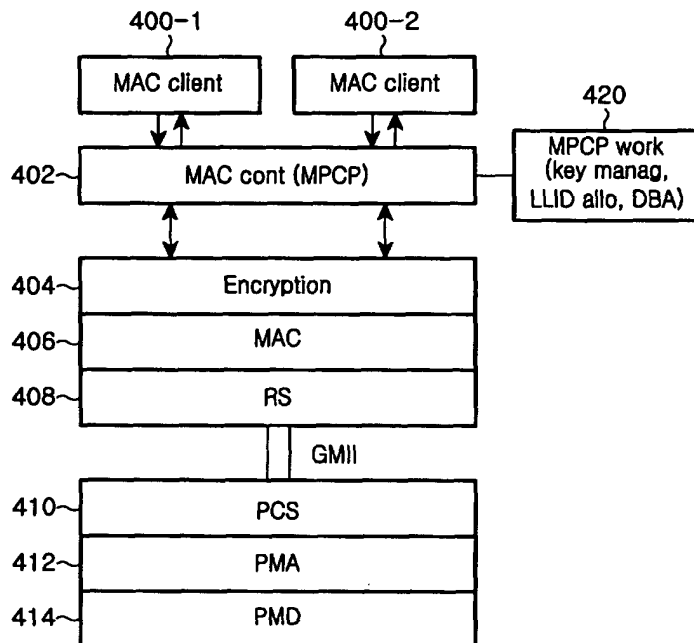
【도 2】



【도 3】



【도 4】



【도 5】

